Release Notes

/ ForgeRock Identity Gateway 6

Latest update: 6.0.0

Mark Craig
Joanne Henry

ForgeRock AS
201 Mission St., Suite 2900
San Francisco, CA 94105, USA
+1 415-599-1100 (US)
www.forgerock.com

Abstract

Notes on prerequisites, fixes, and known issues for the ForgeRock® Identity Gateway.

Table of Contents

Preface

ForgeRock Identity Platform™ serves as the basis for our simple and comprehensive Identity and Access Management solution. We help our customers deepen their relationships with their customers, and improve the productivity and connectivity of their employees and partners. For more information about ForgeRock and about the platform, see https://www.forgerock.com.

Chapter 1
What's New

IG 6 provides many new features and improvements.

1.1. New Features

This release of IG includes the following new features:

ReverseProxyHandler to Stream Responses from a Proxied Application to the User Agent

When IG fails to connect to a proxied application, the ReverseProxyHandler changes the runtime exception into a 502 Bad Gateway response.

When streaming is enabled, responses are processed as soon as all headers are received. The entity content is downloaded in a background thread. This mode reduces latency, and is mandatory for Server-Sent Events (SSE) and the support of very large files (bigger than 2 GB).

For more information, see ReverseProxyHandler(5) in the *Configuration Reference*.

UserProfileFilter to Retrieve Profile Attributes of an AM User

A new filter, UserProfileFilter, queries AM to retrieve the profile attributes of an AM user. It makes the data available as a new context to downstream IG filters and handlers.

For more information, see UserProfileFilter(5) in the *Configuration Reference*.

New SessionInfoFilter Collects Information About the AM Session and Makes it Available to Downstream Handlers

A new filter, SessionInfoFilter, calls the AM endpoint for session information, and makes the data available as a new context to downstream IG filters and handlers. Session properties that are whitelisted in AM are available.

For more information, see SessionInfoFilter(5) in the *Configuration Reference*.

Support for Cross-Domain Single Sign-On

The CrossDomainSingleSignOnFilter, CdSsoContext and CdSsoFailureContext have been added. Users can authenticate to AM in one domain, and then access resources protected by IG in another domain, without having to re-authenticate.

For more information, see "About CDSSO Using the CrossDomainSingleSignOnFilter" in the *Gateway Guide* and CrossDomainSingleSignOnFilter(5) in the *Configuration Reference*.

Updated Monitoring

The Prometheus Scrape Endpoint and Forgerock Common REST Monitoring Endpoint have been added for monitoring.

The endpoints are available in IG, without any configuration. Metrics are available for each router, subrouter, and route in the configuration, and for the defaultHandler of the main router.

By default, everyone has read access to the Prometheus endpoint. No special credentials or privileges are required, but access can be restricted.

For more information, see "*Monitoring*" in the *Gateway Guide*.

AmService Heap Object to Hold Configuration Information About AM

The AmService heap object can be declared in the IG configuration to hold information about an instance of AM.

IG objects that communicate with AM can share AmService, reducing the number of configuration properties in their configuration. For a list of IG objects that can use AmService, see "Deprecated Configuration Settings".

For information, see AmService(5) in the *Configuration Reference*

1.2. Product Improvements

This release of IG includes the following improvements:

Agentless AM Password Capture and Replay

The new CapturedUserPasswordFilter makes it possible to use AM's password capture and replay feature without an AM policy agent.

This filter retrieves an AM password, decrypts it, and exposes it in a new context. By using CapturedUserPasswordFilter, you can get login credentials from AM without setting up an AM policy agent.

From AM 6, CapturedUserPasswordFilter can use the stronger algorithm AES to decrypt the AM password.

For more information, see "*Getting Login Credentials From AM*" in the *Gateway Guide*, and CapturedUserPasswordFilter(5) in the *Configuration Reference*.

Introduction of Session Token Cache

AmService provides a shared session service that can cache session tokens info for improved performance.

IG can now receive notifications from AM on session log out, or when an AM session is modified, closed, is destroyed, or times out. IG evicts related entries from the session cache.

SingleSignOnFilter, CrossDomainSingleSignOnFilter, SessionInfoFilter, UserProfileFilter and PolicyEnforcementFilter are using that shared service.

In previous releases, the SingleSignOnFilter called AM to validate the SSO token for every request in a session. The SingleSignOnFilter can now process multiple requests in the same session without calling AM to validate the SSO token.

For more information, see AmService(5) in the *Configuration Reference* and "Enable Websocket Notifications" in the *Configuration Reference*.

Eviction From the PolicyEnforcementFilter Cache

IG can now capture WebSocket notifications from AM when a policy is created, deleted, or updated, and then clear the PolicyEnforcementFilter cache. To facilitate this feature, the PolicyEnforcementFilter cache has been replaced by a cache based on *Caffeine*.

For more information, see "Enable Websocket Notifications" in the *Configuration Reference*. For more information about Caffeine, see the GitHub entry, *Caffeine*.

More Configuration Options for Caching for OAuth 2.0 access_tokens

More options are provided for caching access_tokens in OAuth2ResourceServerFilter.

Faster Response Processing and Processing for Response Sizes Over 2 GB

From this release, when streaming is enabled on the ClientHandler or ReverseProxyHandler, IG begins streaming a response to a client as soon as it begins receiving it from the downstream application.

Because IG does not need to buffer the entire content of the response, it can process responses faster, and can proxy applications and APIs that send responses bigger than 2 GB.

If the response flow includes a filter that buffers the entire content of the response, such as capture decorator, processing takes longer and the maximum size of the response is 2 GB.

AM Realm Containing UMA Configuration Can be Specified

The AM realm that contains the UMA configuration can be specified in UmaService.

The endpoint for an UMA sharing service is now configured by the `wellKnownEndpoint` property of UmaService instead of `authorizationServerUri`. `authorizationServerUri` has been removed.

For more information, see UmaService(5) in the *Configuration Reference*.

Support for Additional Advice Types in PolicyEnforcementFilter

The PolicyEnforcementFilter now supports the following AM advice types in addition to `AuthLevel`:

- `AuthenticateToService`
- `AuthenticateToRealm`
- `AuthScheme`

For more information, see PolicyEnforcementFilter(5) in the *Configuration Reference*.

IG Can Use System-Defined Proxy Server

IG can now make use of a system-defined proxy server. Use the new `systemProxy` property of ClientHandler and ReverseProxyHandler to access the feature.

For more information, see ClientHandler(5) in the *Configuration Reference* and ReverseProxyHandler(5) in the *Configuration Reference*.

Support for Parameterized Configuration

Support for parameterized configuration has been added through the introduction of configuration tokens, and the processes of token resolution, JSON evaluation, token substitution, and data transformation.

At startup and when routes are loaded, token resolvers make values available from environment variables, Java system properties, JSON and Java properties files, and route properties. Matching values are substituted in the configuration files as strings, and then transformed as required into different data types.

For more information, see Property Value Substitution in the *Configuration Reference*.

IG Can Proxy SSE API

IG can now proxy Server Sent Events (SSE) API.

Captured Entity Size Is Limited

The CaptureDecorator property `maxEntityLength` has been added to limit the number of bytes that can be captured for an entity. Before this release, IG tried to capture the entire entity.

When the CaptureDecorator property `captureEntity` is `true`, use this property to prevent excessive memory use or `OutOfMemoryError` errors.

For information, see CaptureDecorator(5) in the *Configuration Reference*.

IG Is Automatically Deployed On the Root Context In Jetty

To deploy IG in Jetty, it is no longer necessary to rename the IG .war file from `IG-6.0.0.war` to `root.war`.

For more information, see "Installing and Starting IG" in the *Getting Started Guide*.

Class Import for Groovy Scripts

The following additional classes are now imported automatically for Groovy scripts:

- `org.forgerock.http.oauth2.AccessTokenInfo`
- `org.forgerock.json.JsonValue`

It is no longer necessary to include imports statements for these classes in Groovy scripts.

IG Can Retry HTTP Requests On Connection Failure

IG can now retry failed HTTP requests. You can specify the number of times IG retries a failed request, and the delay between retries.

In bootstrapping scenarios where IG depends on third-party services, IG can now pause the startup process until the required services are online (ex: OpenID Connect well-know configuration endpoint).

For more information, see ClientHandler(5) in the *Configuration Reference*.

Studio

Studio has been updated to include the following features:

Technology Preview of Freeform Studio

Freeform Studio is a new user interface to develop complex routes of filters and handlers. As you design a route, Freeform Studio helps you to visualize the chain of filters and handlers, identify break points, and track the path of requests, responses, and contexts.

Freeform Studio is offered as Technology Preview, as defined in "*Release Levels and Interface Stability*".

For more information and some pointers for getting started with Freeform Studio, see "*Technology Preview of Freeform Studio*" in the *Getting Started Guide*.

Configuration for TokenTransformationFilter

The TokenTransformationFilter can now be configured in Studio.

For an example configuration, see "To Set Up IG For Token Transformation" in the *Gateway Guide*.

Use of Arguments in Scripts

Scripts for use in the ScriptableFilter and ThrottlingFilter can now be configured with arguments in Studio.

For an example configuration, see " Configuring a Scriptable Throttling Filter " in the *Gateway Guide*.

Audit Logging With JSON Audit Event Handler and ElasticSearch Audit Handler

Audit logging can now be configured in Studio for JSON audit event handler and ElasticSearch audit event handler.

For more information, see "Recording Audit Events in JSON" in the *Gateway Guide*.

Configuration for Stateless Sessions

Stateless sessions that do not use a keystore can now be configured in Studio.

For more information, see "To Create a Route With Advanced Options" in the *Getting Started Guide* and JwtSession(5) in the *Configuration Reference*.

Assisted Upgrade for Routes Deployed in Studio

During IG upgrade, routes that were previously created in Studio are automatically transferred to the new version of IG. If extra information is required for compatibility, you are prompted for the required information.

For more information, see ⚠ Compatibility update required in the "Route Status" in the *Getting Started Guide*.

Capture Message Context in Studio

Studio can now be used to configure the capture of the message context as well as the message body.

For information, see "Capturing Log Messages for Routes" in the *Gateway Guide*

1.3. Security Advisories

ForgeRock issues security advisories in collaboration with our customers and the open source community to address any security vulnerabilities transparently and rapidly. ForgeRock's security advisory policy governs the process on how security issues are submitted, received, and evaluated as well as the timeline for the issuance of security advisories and patches.

For details of all the security advisories across ForgeRock products, see Security Advisories in the *Knowledge Base library*.

Chapter 2
Before You Install

This chapter describes the requirements for running IG.

Tip

If you have a request to support a component or combination not listed here, contact ForgeRock at info@forgerock.com.

2.1. Downloading IG Software

Download the following product software from the ForgeRock BackStage download site:

- IG .war file, `IG-6.0.0.war`
- Web application for testing IG configurations, `IG-sample-application-6.0.0.jar`

2.2. JDK Version

IG runs with the following JDKs:

- Oracle JDK 8
- OpenJDK 1.8

  If you are using IG on Tomcat with SSL enabled, use OpenJDK 1.8.0_121 or later versions to prevent mismatch between client side ciphers and server side ciphers.

For the latest security fixes, ForgeRock recommends that you use the most recent update.

If you install an AM policy agent in the same container as IG, you must use a Java release that is also supported by that policy agent.

2.3. Web Application Containers

IG runs in the following web application containers:

- Apache Tomcat 8 or 8.5.x
- Jetty 9.3.x or later version
- JBoss EAP 7

Deploy IG to the root context of the container. Deployment in other contexts causes unexpected results, and is not supported.

For information about setting up a web application container see "Configuring Deployment Containers" in the *Gateway Guide*.

2.4. Features Supported With ForgeRock Access Management

This section describes the IG features that are supported with AM:

Features Supported With AM

Feature	**Supported In AM Version**
Eviction of entries from the AmService `sessionCache`, using WebSocket notifications from AM. For more information, see AmService(5) in the *Configuration Reference*.	AM 6, and AM 5.5 when the `AMCtxId` session property is whitelisted
AM password capture and replay, as described in "*Getting Login Credentials From AM*" in the *Gateway Guide*.	AM 5 and later
AM policy enforcement, as described in "*Enforcing Policy Decisions and Supporting Session Upgrade*" in the *Gateway Guide*.	AM 5 and later
OpenID Connect dynamic registration and discovery, as described in "Using OpenID Connect Discovery and Dynamic Client Registration" in the *Gateway Guide*.	OpenAM 13.5.x, and AM 5 and later
Token transformation, as described in "*Transforming OpenID Connect ID Tokens Into SAML Assertions*" in the *Gateway Guide*.	OpenAM 13.5.x, and AM 5 and later
User Managed Access 2.x, for IG 5.5, as described in "*Supporting UMA Resource Servers*" in the *Gateway Guide*.	AM 5.5 and later
User Managed Access 1.x, for IG 5 and earlier versions.	AM 5.1 and earlier
Single sign-on, as described in "About SSO Using the SingleSignOnFilter" in the *Gateway Guide*.	AM 5 and later
Cross-domain single sign-on, as described in "About CDSSO Using the CrossDomainSingleSignOnFilter" in the *Gateway Guide*.	AM 5.5 and later

Feature	**Supported In AM Version**
Capture and storage of AM session information, as described in SessionInfoFilter(5) in the *Configuration Reference*.	AM 5 and later
Capture and storage of AM user profile attributes, as described in UserProfileFilter(5) in the *Configuration Reference*.	AM 5 and later

2.5. ForgeRock Access Management Policy Agents

When installing an AM policy agent in the same container as IG, use AM Java EE Policy Agent 3.5 or later. Earlier versions might not shut down properly with the web application container.

Make sure that the container version is supported both for IG and the AM Java EE Policy Agent that you install alongside IG.

AM Java EE Policy Agent 3.5.1 and earlier versions do not support Tomcat 8.5.x or Jetty 9.

Chapter 3 Compatibility With Other Releases

This chapter describes major changes to existing functionality, deprecated functionality, and removed functionality.

3.1. Important Changes to Existing Functionality

This release of IG includes the following important change:

Production Mode by Default

By default, after installation IG is now in production (immutable) mode instead of development (mutable) mode. To use Studio and manage routes through Common REST, you must switch to development mode.

For information about modes and switching to development mode, see "Switching Between Production Mode and Development Mode" in the *Getting Started Guide*.

Introduction of ReverseProxyHandler

The chain in routes created in Studio now ends with a ReverseProxyHandler instead of a ClientHandler.

For information, see ReverseProxyHandler(5) in the *Configuration Reference*.

PolicyEnforcementFilter Credentials Must Be Registered as Java Agent

It is now mandatory to register an AM Java agent in order to use the PolicyEnforcementFilter.

The tokens issued by AM for an agent have an unlimited lifetime (unless configured otherwise), and all appropriate permissions, making them a perfect fit for an application needing to ask for policy decisions.

For information, see PolicyEnforcementFilter(5) in the *Configuration Reference*.

ClientHandler Verifies the Hostname for Outgoing SSL Connections

By default, the ClientHandler now verifies the hostname for outgoing SSL connections. By default, in previous releases the hostname was not verified.

For more information, see the `hostnameVerifier` property in ClientHandler(5) in the *Configuration Reference*.

Route Filename, Name, and ID

The filename of a route cannot be `default.json`, and the route's `name` property and route ID cannot be `default`.

For more information, see " Creating and Editing Routes Through Common REST " in the *Gateway Guide* and Route(5) in the *Configuration Reference*.

Servlet 2.x Support Removed

This release supports servlet 3.x. Servlet 2.x is no longer supported.

Captured Entity Size Is Limited

By default, when the CaptureDecorator property `captureEntity` is `true`, up to 512 KB of an entity can be captured. Before this release, IG tried to capture the entire entity.

The CaptureDecorator property `maxEntityLength` has been added to limit the maximum size of captured entities, and so prevent excessive memory use or `OutOfMemoryError`. For information, see CaptureDecorator(5) in the *Configuration Reference*.

ApiProtectionFilter protects `/openig/api`

The default ApiProtectionFilter now protects the `/openig/api` endpoint. Before this release, it protected the `/openig` endpoint.

Plus (`+`) Not Allowed in Names

The plus character, `+`, is now a reserved character in names.

The `+` character is no longer allowed in object and route names.

Timestamp In Route Log Files Complies With ISO 8601

The timestamp in route logs now includes the date, and is compliant with ISO 8601. The following examples show the impact of this change on log parsing:

- An entry in the route log was previously in this format:

```
10:57:12:158 | INFO  | openig.example.com-startStop-1  . . .
```

- The entry now appears in this format:

```
2018-01-16T10:57:12,242Z | INFO  | openig.example.com-startStop-1  . . .
```

3.2. Deprecated Functionality

During IG upgrade, routes that were previously created in Studio are automatically transferred to the new version of IG. Where possible, IG replaces deprecated settings with the newer evolved setting. If IG needs additional information to upgrade the route, the route status becomes ⚠ Compatibility update required. Select the route and provide the requested information.

This section lists deprecated functionality. Deprecation is defined in "ForgeRock Product Interface Stability".

IG Route Monitoring Endpoint

The IG Route Monitoring Endpoint is deprecated in this release and will be removed in the next release. As a replacement, IG provides Prometheus Scrape Endpoint and Forgerock Common REST Monitoring Endpoint.

For more information, see "Prometheus Scrape Endpoint" in the *Gateway Guide*, and "Forgerock Common REST Monitoring Endpoint" in the *Gateway Guide*,

Support for .war File Delivery

The delivery of a .war file is deprecated in this release and may be removed in the next release.

Support AM Policy Agents

Support for the use of AM policy agents in password capture and replay is deprecated in this release.

By using CapturedUserPasswordFilter, you can get login credentials from AM without setting up an AM policy agent. For more information, see "*Getting Login Credentials From AM*" in the *Gateway Guide*, and CapturedUserPasswordFilter(5) in the *Configuration Reference*.

Deprecated Configuration Settings

Configuration Object	Deprecated Settings	Replacement Settings
The environment variable and system property that define the file system directory for configuration files.	`OPENIG_BASE` and `openig.base`	Replaced by `IG_INSTANCE_DIR` and `ig.instance.dir` If neither the deprecated setting nor the replacement setting are provided, configuration files are in the default directory `$HOME/.openig` (on Windows, `%appdata%\OpenIG`). If the deprecated setting and the replacement setting are both provided, the replacement setting is used.
OpenAmAccessTokenResolver	`endpoint`	Replaced by the AmService property `url`. For information, see OpenAmAccessTokenResolver in OAuth2ResourceServerFilter(5) in the *Configuration Reference*.
PolicyEnforcementFilter	`amHandler`, `openamUrl`, `realm`, and `ssoTokenHeader`	Replaced by the AmService properties `amHandler`, `url`, `realm`, and `ssoTokenHeader`

Configuration Object	Deprecated Settings	Replacement Settings
	`cache` property `maxTimeout`	Replaced by `cache` property `maximumTimeToCache`
SingleSignOnFilter	`amHandler`, `openamUrl`, `realm`, and `cookieName`	Replaced by the AmService properties `amHandler`, `url`, `realm`, and `ssoTokenHeader` For information, see SingleSignOnFilter(5) in the *Configuration Reference*.
TokenTransformationFilter	`amHandler`, `openamUri`, `realm`, and `ssoTokenHeader`	Replaced by the AmService properties `amHandler`, `url`, `realm`, and `ssoTokenHeader`. For information, see TokenTransformationFilter(5) in the *Configuration Reference*.
`OAuth2ResourceServerFilter`	`cacheExpiration`	Replaced by `cache` and its sub-properties `enabled`, `defaultTimeout`, and `maxTimeout`. If `cacheExpiration` is configured and `cache` is not configured, the cache is enabled and the value of `cacheExpiration` is used as `maxTimeout`. The following values for `cacheExpiration`, supported in previous releases, are not supported in this release: `zero`, `unlimited`. For more information, see OAuth2ResourceServerFilter(5) in the *Configuration Reference*.

3.3. Removed Functionality

This section lists removed functionality. Removed is defined in "ForgeRock Product Interface Stability".

HeapClientRegistrationRepository

The class `HeapClientRegistrationRepository` is removed from this release. Declare client registrations in the `registrations` attribute of OAuth2ClientFilter.

Support for Jetty 8

Support for Jetty 8 has been removed in this release.

Use Jetty 9 instead.

Removed Configuration Settings

Configuration Object	Removed Settings	Newer Evolving Settings
UmaService	`authorizationServerUri`	Replaced by `wellKnownEndpoint` and the AmService property `url`. For more information, see UmaService(5) in the *Configuration Reference*.
`OpenAmAccessTokenResolver`	`endpoint`	`amService`
ClientRegistration	`tokenEndpointUseBasicAuth`	Replaced by `tokenEndpointAuthMethod`. `"tokenEndpointAuthMethod": "client_secret_post"` is equivalent to `"tokenEndpointUseBasicAuth": false`. `"tokenEndpointAuthMethod": "client_secret_basic"` is equivalent to `"tokenEndpointUseBasicAuth": true`. For information, see ClientRegistration(5) in the *Configuration Reference*.
OAuth2ResourceServerFilter	`tokenInfoEndpoint` and `providerHandler`	Replaced by configuration properties of OpenAmAccessTokenResolver, TokenIntrospectionAccessTokenResolver, and ScriptableAccessTokenResolver. For information, see OAuth2ResourceServerFilter(5) in the *Configuration Reference*.

Chapter 4

Fixes, Limitations, and Known Issues

IG issues are tracked at https://bugster.forgerock.org/jira/browse/OPENIG. This chapter covers the status of key issues and limitations at release 6.

4.1. Key Fixes

This release of IG fixes the following important issues:

- OPENIG-2571: OAuth2ResourceServerFilter requireHttps=true applies to rebased request URI
- OPENIG-2565: PolicyEnforcementFilter returns 403 instead of 401 when route is accessed with an unauthenticated user
- OPENIG-2220: PasswordReplayFilter : automatic login fails due to SSLPeerUnverifiedException although ClientHandler is configured with a TrustAllManager
- OPENIG-2149: CREST resource filtering should not alter structure of resource
- OPENIG-2004: OAuth2ResourceServerFilter cache configuration can lead to unexpected results if tokens expire early
- OPENIG-1325: Cannot specify realm in UmaService
- OPENIG-816: The UmaResourceServerFilter returns with wrong as_uri

4.2. Limitations

This release of IG includes the following limitations:

systemProxy Can't Be Used With Proxy Requiring Username and Password

> The ClientHandler and ReverseProxyHandler property `systemProxy` can't be used with a proxy that requires a username and password. Use the handler's `proxy` property instead.
>
> For more information, see the `agent` property of ClientHandler(5) in the *Configuration Reference* and ReverseProxyHandler(5) in the *Configuration Reference*.

Fail To Receive AM WebSocket Notifications with Jetty

When IG runs on versions of Jetty from 9.3.x to 9.4.8, WebSocket notifications are not received correctly. To work around this issue, comment out the entry `-module=websocket` in Jetty's `start.ini` file.

For more information, see the `agent` property of AmService(5) in the *Configuration Reference*.

Support for UMA Is Experimental

IG provides experimental support for building a UMA resource server, with the capability and limitations described in "*Supporting UMA Resource Servers*" in the *Gateway Guide*.

For Studio, Custom `config.json` Must Contain Main Router Named `_router`

Studio deploys and undeploys routes through a main router named `_router`, which is the name of the main router in the default configuration. If you use a custom `config.json`, make sure that it contains a main router named `_router`.

For information, see "Creating Routes Through Studio " in the *Gateway Guide*.

Log File of Audit Events Can be Overwritten

The log file of audit events can be overwritten when the log file is rotated.

When `CsvAuditEventHandler` is used to log audit events, the log file is overwritten if it is rotated before the file suffix, `rotationFileSuffix`, changes. By default, `rotationFileSuffix` is defined as a date in the format `_yyyy-MM-dd`.

Log files are rotated when one of the following limits is reached: `maxFileSize`, `rotationInterval`, or `rotationTimes`.

Set the log rotation parameters so that the log is not likely to rotate before `rotationFileSuffix` changes.

For Mutual Authentication, Client Certificate Must Be First in KeyStore

For HTTPS, IG can check server certificates. However, mutual authentication, where IG presents its client certificate, is not supported if the client certificate is not the first certificate in the ClientHandler or ReverseProxyHandler keystore.

IG Scripts Can Access Anything in Their Environment

IG scripts are not sandboxed, but instead have access to anything in their environment. You must make sure that the scripts that IG loads are safe.

`SamlFederationHandler` Doesn't Support Filtering

The `SamlFederationHandler` does not support filtering. Do not use a `SamlFederationHandler` as the handler for a `Chain`.

More generally, do not use this handler when its use depends on something in the response. The response can be handled independently of IG, and can be `null` when control returns to IG. For example, do not use this handler in a `SequenceHandler` where the `postcondition` depends on the response.

`CookieFilter` is not JwtSession compatible

The CookieFilter heap object stores a java.net.CookieManager reference in the `session`, so that cookies are linked to the HTTP session. This behavior is not compatible with the use of a JwtSession.

SAML v2.0 Federation does not work if the user defined mapping is incorrectly set

If the user defined mapping is incorrectly set, missing SAML assertions produce an infinite loop during authentication attempts.

4.3. Known Issues

This release of IG includes the following known issues:

- OPENIG-2144: AuditService and JmsAuditEventHandler : failure on Jboss
- OPENIG-1628: Script update referenced in route, not taken into account
- OPENIG-1557: UI: Unable to deploy route when custom router is configured
- OPENIG-813: auditService : fileRotation may overwrite existing audit file
- OPENIG-659: CryptoHeaderFilter - error on handling header value with incorrect length

Chapter 5
Documentation Changes

This release of IG includes the following changes to the documentation:

- 2020-04-15: Correction to the `AMCtxId` property name.
- 2020-04-15: Minor correction in SAML routes with multiple service providers.
- 2019-05-28: Minor correction in SingleSignOnFilter.
- The ClientHandler property `disableRetries` has been removed from the documentation. This property is ignored in OpenIG 4.5 and later versions, since the introduction of asynchronous processing for filters and handlers.
- From this release, you can configure AM's password capture and replay without setting up an AM policy agent. In "*Getting Login Credentials From AM*" in the *Gateway Guide*, the example that uses an AM policy agent has been replaced with an example that uses CapturedUserPasswordFilter. For information about using an AM policy agent, see the documentation for earlier versions of IG.
- The `PolicyEnforcementFilter` now requires policy agent credentials. You must set up a Java agent profile for the filter in AM, rather than using the `policyAdmin` account. For details, see "*Enforcing Policy Decisions and Supporting Session Upgrade*" in the *Gateway Guide* and PolicyEnforcementFilter(5) in the *Configuration Reference*.
- Information about monitoring is in a new chapter, "*Monitoring*" in the *Gateway Guide*. Monitoring metrics have been added in Monitoring in the *Configuration Reference*.

Appendix A. Release Levels and Interface Stability

This appendix includes ForgeRock definitions for product release levels and interface stability.

A.1. ForgeRock Product Release Levels

ForgeRock defines Major, Minor, Maintenance, and Patch product release levels. The release level is reflected in the version number. The release level tells you what sort of compatibility changes to expect.

Release Level Definitions

Release Label	Version Numbers	Characteristics
Major	Version: x[.0.0] (trailing 0s are optional)	• Bring major new features, minor features, and bug fixes • Can include changes even to Stable interfaces • Can remove previously Deprecated functionality, and in rare cases remove Evolving functionality that has not been explicitly Deprecated • Include changes present in previous Minor and Maintenance releases
Minor	Version: x.y[.0] (trailing 0s are optional)	• Bring minor features, and bug fixes

Release Label	Version Numbers	Characteristics
		• Can include backwards-compatible changes to Stable interfaces in the same Major release, and incompatible changes to Evolving interfaces • Can remove previously Deprecated functionality • Include changes present in previous Minor and Maintenance releases
Maintenance, Patch	Version: x.y.z[.p] The optional `.p` reflects a Patch version.	• Bring bug fixes • Are intended to be fully compatible with previous versions from the same Minor release

A.2. ForgeRock Product Interface Stability

ForgeRock products support many protocols, APIs, GUIs, and command-line interfaces. Some of these interfaces are standard and very stable. Others offer new functionality that is continuing to evolve.

ForgeRock acknowledges that you invest in these interfaces, and therefore must know when and how ForgeRock expects them to change. For that reason, ForgeRock defines interface stability labels and uses these definitions in ForgeRock products.

Interface Stability Definitions

Stability Label	Definition
Stable	This documented interface is expected to undergo backwards-compatible changes only for major releases. Changes may be announced at least one minor release before they take effect.
Evolving	This documented interface is continuing to evolve and so is expected to change, potentially in backwards-incompatible ways even in a minor release. Changes are documented at the time of product release. While new protocols and APIs are still in the process of standardization, they are Evolving. This applies for example to recent Internet-Draft implementations, and also to newly developed functionality.
Deprecated	This interface is deprecated and likely to be removed in a future release. For previously stable interfaces, the change was likely announced in a previous release. Deprecated interfaces will be removed from ForgeRock products.
Removed	This interface was deprecated in a previous release and has now been removed from the product.
Technology Preview	Technology previews provide access to new features that are evolving new technology that are not yet supported. Technology preview features may be functionally incomplete and the function as implemented is subject to

Stability Label	Definition
	change without notice. DO NOT DEPLOY A TECHNOLOGY PREVIEW INTO A PRODUCTION ENVIRONMENT. Customers are encouraged to test drive the technology preview features in a non-production environment and are welcome to make comments and suggestions about the features in the associated forums. ForgeRock does not guarantee that a technology preview feature will be present in future releases, the final complete version of the feature is liable to change between preview and the final version. Once a technology preview moves into the completed version, said feature will become part of the ForgeRock platform. Technology previews are provided on an “AS-IS” basis for evaluation purposes only and ForgeRock accepts no liability or obligations for the use thereof.
Internal/Undocumented	Internal and undocumented interfaces can change without notice. If you depend on one of these interfaces, contact ForgeRock support or email info@forgerock.com to discuss your needs.

Appendix B. Getting Support

This chapter includes information and resources for IG and ForgeRock support.

B.1. Accessing Documentation Online

ForgeRock publishes comprehensive documentation online:

- The ForgeRock Knowledge Base offers a large and increasing number of up-to-date, practical articles that help you deploy and manage ForgeRock software.

  While many articles are visible to community members, ForgeRock customers have access to much more, including advanced information for customers using ForgeRock software in a mission-critical capacity.

- ForgeRock product documentation, such as this document, aims to be technically accurate and complete with respect to the software documented. It is visible to everyone and covers all product features and examples of how to use them.

B.2. How to Report Problems or Provide Feedback

If you find issues or reproducible bugs, report them in https://bugster.forgerock.org.

When requesting help with a problem, include the following information:

- Description of the problem, including when the problem occurs and its impact on your operation
- Description of the environment, including the following information:

  - Machine type
  - Operating system and version
  - Web server or container and version
  - Java version
  - Patches or other software that might affect the problem
- Steps to reproduce the problem
- Relevant access and error logs, stack traces, and core dumps

B.3. Getting Support and Contacting ForgeRock

ForgeRock provides support services, professional services, training through ForgeRock University, and partner services to assist you in setting up and maintaining your deployments. For a general overview of these services, see https://www.forgerock.com.

ForgeRock has staff members around the globe who support our international customers and partners. For details, visit https://www.forgerock.com, or send an email to ForgeRock at info@forgerock.com.